PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-303114
(43)Date of publication of application : 24.10.2003

(51)Int.Cl. G06F 11/00
G06F 1/00
G06F 9/445
G06K 17/00

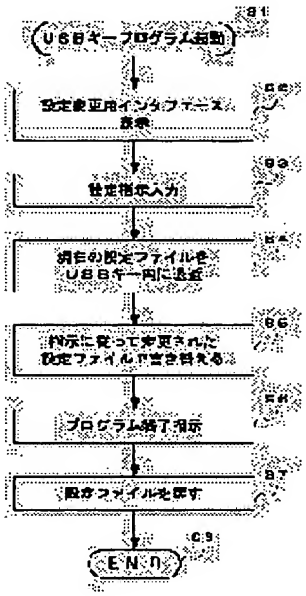
(21)Application number : 2002-317984
(22)Date of filing : 31.10.2002

(71)Applicant : CLKK
(72)Inventor : HATA ATSUSHI

(30)Priority
Priority number : 2002029168 Priority date : 06.02.2002 Priority country : JP

(54) SECURITY MAINTENANCE SYSTEM AND USB KEY

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a security maintenance system and a USB key capable of easily changing settings of a browser and a mailer for preventing invasion of a computer virus according to a security level, diagnosing a security hole condition in compliance with a personal computer condition, and easily applying a patch to the security hole.
SOLUTION: In this security maintenance system and the USB key, a program inside the USB key changes settings of the browser and the mailer according to a security level and checks a PC condition to output it to a Web server 3. The Web server 3 diagnoses whether the latest patch is applied in compliance with the PC condition or not, displays the diagnosis result to the PC, and urges that the patch should be applied according to guidance if the patch is not applied.



【図2】

LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－303114
（P2003－303114A）
(43)公開日　平成15年10月24日(2003.10.24)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　11/00		Ｇ０６Ｋ　17/00	Ｌ	５Ｂ０５８
1/00		Ｇ０６Ｆ　9/06	６６０Ｎ	５Ｂ０７６
9/445			６５０Ｋ	
Ｇ０６Ｋ　17/00			６３０Ｂ	
			６６０Ｚ	

審査請求　未請求　請求項の数15　ＯＬ　（全 11 頁）

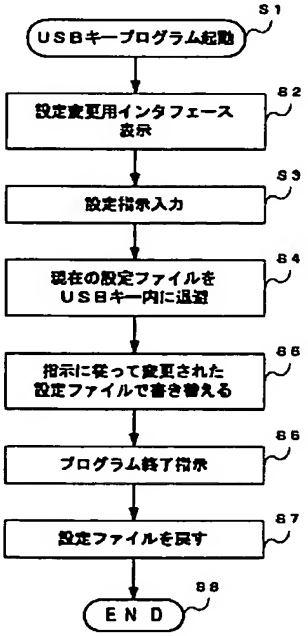
(21)出願番号　特願2002－317984(P2002－317984)
(22)出願日　平成14年10月31日(2002.10.31)
(31)優先権主張番号　特願2002－29168(P2002－29168)
(32)優先日　平成14年２月６日(2002.2.6)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　301068930
株式会社シーアイ
東京都豊島区池袋二丁目43番１号　池袋青柳ビル10Ｆ
(72)発明者　畑　温
東京都豊島区池袋二丁目43番１号　池袋青柳ビル10Ｆ　株式会社シーアイ内
(74)代理人　100093104
弁理士　船津　暢宏　（外１名）

Ｆターム(参考)　5B058 CA01 CA27 KA02 KA21 KA31 YA13
5B076 BA10 BB04 BB18 BB19 EA01

(54)【発明の名称】　セキュリティ保全システム及びＵＳＢキー

(57)【要約】
【課題】　本発明は、コンピュータウィルスの侵入防止のために、ブラウザー及びメーラーの設定をセキュリティのレベルに応じて容易に変更でき、パソコンの状態に応じてセキュリティホールの状況を診断し、そのセキュリティホールに対して容易にパッチを当てることができるセキュリティ保全システム及びＵＳＢキーを提供する。
【解決手段】　ＵＳＢキー内のプログラムが、ブラウザー及びメーラーの設定をセキュリティのレベルに応じて変更し、またＰＣの状態をチェックしてＷｅｂサーバ３に出力し、Ｗｅｂサーバ３は、当該ＰＣ状態に応じて最新のパッチが当てられているか否かを診断してＰＣ向けに表示し、パッチが当てられていなければガイダンスに従ってパッチを当てるよう促すセキュリティ保全システム及びＵＳＢキーである。



【図2】

1

【特許請求の範囲】

【請求項１】　コンピュータのＵＳＢポートに接続されるＵＳＢキーであって、

前記ＵＳＢポートに前記ＵＳＢキーが差し込まれた状態で、前記コンピュータに搭載されているブラウザー又はメーラー若しくは双方のセキュリティに関する設定ファイルを退避し、予め用意されたセキュリティを向上させる設定ファイルに変更し、前記ＵＳＢキーを前記ＵＳＢポートから抜き出す際の処理において変更した設定ファイルを前記退避した設定ファイルに戻すコンピュータプログラムを記録することを特徴とするＵＳＢキー。

【請求項２】　変更可能な設定ファイルが、ユーザの指定により設定事項をセキュリティの程度に応じて変更可能であることを特徴とする請求項１記載のＵＳＢキー。

【請求項３】　コンピュータのＵＳＢポートに接続されるＵＳＢキーであって、

前記ＵＳＢポートに前記ＵＳＢキーが差し込まれた状態で、コンピュータに搭載されたＯＳの状態をチェックし、当該ＯＳに関する情報を予め記憶するＵＲＬのサイトに接続し、前記情報を前記サイトのウェブサーバに出力するコンピュータプログラムを記憶することを特徴とするＵＳＢキー。

【請求項４】　請求項３記載のＵＳＢキーから提供されたＯＳに関する情報に対して、当該ＯＳのセキュリティホールに最新のパッチが当てられているか否かを診断し、最新のパッチが当てられていればその旨を表示し、最新のパッチが当てられていなければ当該パッチを当てるためのガイダンスを表示するウェブサーバを有することを特徴とするセキュリティ保全システム。

【請求項５】　ＵＳＢキーがコンピュータのＵＳＢポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、前記コンピュータは前記ＵＳＢキー内に記憶するＵＲＬにアクセスしてＯＳに関する情報をウェブサーバに提供することを特徴とする請求項４記載のセキュリティ保全システム。

【請求項６】　ウェブサーバは、表示の際に、セキュリティホールに関する情報、コンピュータウィルス及びワクチンソフトに関する情報も表示することを特徴とする請求項４又は５記載のセキュリティ保全システム。

【請求項７】　コンピュータのＵＳＢポートに接続されるＵＳＢキーであって、

前記ＵＳＢポートに前記ＵＳＢキーが差し込まれた状態で、前記コンピュータに搭載されているブラウザー又はメーラー若しくは双方のセキュリティに関する設定ファイルをコピーし、当該ＵＳＢキー内に記憶するＵＲＬにアクセスして当該コンピュータのＯＳに関する情報及びコピーした設定ファイルをウェブサーバに提供し、前記ＯＳに関する情報と前記コピーした設定ファイルから前記ウェブサーバが用意したセキュリティに関する設定ファイルを前記コンピュータで使用可能とするコンピュータプログラムを記録することを特徴とするＵＳＢキー。

2

【請求項８】　請求項７記載のＵＳＢキーから提供されたＯＳに関する情報及びコピーした設定ファイルに対して、当該ＯＳに関する情報に対して当該コピーした設定ファイルがセキュリティ確保できる内容であるか判断し、セキュリティ確保できないものであれば、セキュリティ確保できる設定ファイルをコンピュータに対して提供するウェブサーバを有することを特徴とするセキュリティ保全システム。

【請求項９】　ＵＳＢキーがコンピュータのＵＳＢポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、前記コンピュータは前記ＵＳＢキー内に記憶するＵＲＬにアクセスしてＯＳに関する情報及びコピーしたセキュリティに関する設定ファイルをウェブサーバに提供することを特徴とする請求項８記載のセキュリティ保全システム。

【請求項１０】　変更する設定ファイルの設定内容は、規定値としてセキュリティが最高レベルとなるよう設定されていることを特徴とする請求項１又は２記載のＵＳＢキー。

【請求項１１】　新規プロセスが発生すると、当該プロセスがレジストリに正規に登録されているか否かを検索し、正規に登録されていれば当該プロセスを動作させ、正規に登録されていなければ当該プロセスを動作させないプロセス監視機能を備えたことを特徴とする請求項１又は２、若しくは請求項１０のいずれか記載のＵＳＢキー。

【請求項１２】　ＯＳに関する情報の問い合わせに対してＯＳに関する情報の出力を停止するロック機能を備えたことを特徴とする請求項１１記載のＵＳＢキー。

【請求項１３】　特定サイトにアクセスし、ファイルのウィルス感染をチェックし、当該ファイルをオンラインバックアップする機能を備えたことを特徴とする請求項１１又は１２記載のＵＳＢキー。

【請求項１４】　コンピュータのシステム領域への不正アクセスを禁止する機能と、新規ファイルの自動作成を禁止する機能と、コンピュータの記憶装置内のファイルへの不正アクセスを禁止する機能とを備えたことを特徴とする請求項１又は２、若しくは請求項１１乃至１３のいずれか記載のＵＳＢキー。

【請求項１５】　コンピュータのメモリ常駐を不許可とした上で、ファイル内容をテキストに変換してコンピュータで表示させる機能を備えたことを特徴とする請求項１４記載のＵＳＢキー。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＵＳＢ（Universal Serial Bus）キーを用いたセキュリティ保全システムに係り、特に、ブラウザー及びメーラーの設定を簡易に変更することでコンピュータウィルスの侵入を防止する

3

と共に、パソコンのＯＳ（Operating System）におけるセキュリティホールにパッチを当てることを手助けするセキュリティ保全システム及びＵＳＢキーに関する。

【０００２】

【従来の技術】インターネットにアクセスした際に、パーソナルコンピュータ（パソコン：ＰＣ）のセキュリティホールを狙って、コンピュータウィルスが侵入することがある。このため、ＯＳ提供会社は、コンピュータウィルスの侵入を防ぐために、そのセキュリティホールにパッチを当てるための情報及びパッチ用プログラムを提供している。

【０００３】

【発明が解決しようとする課題】しかしながら、ＯＳ提供会社の提供する情報に従ったブラウザー及びメーラーの設定変更は、パソコン初心者には難しく、設定変更をうまく行うことができないという問題点があった。また、セキュリティホールにパッチを当てるプログラムは提供されているものの、実際のパッチを当てる作業はパソコン初心者には難しく、容易にパッチを当てることができないという問題点があった。更に、ＰＣユーザは、定期的にＯＳ提供会社の情報にアクセスして自機を最新のセキュリティ保全状態としなければならず、メンテナンスが面倒であるとの問題点があった。

【０００４】本発明は上記実情に鑑みて為されたもので、コンピュータウィルスの侵入を防ぐために、パソコン初心者でもブラウザー及びメーラーの設定をセキュリティのレベルに応じて容易に変更できるＵＳＢキーを提供することを目的とする。

【０００５】また、本発明の別の目的は、パソコンの状態に応じてセキュリティホールの状況を診断し、そのセキュリティホールに対してパソコン初心者でも容易にパッチを当てることができるセキュリティ保全システム及びＵＳＢキーを提供することにある。

【０００６】

【課題を解決するための手段】上記従来例の問題点を解決するための本発明は、コンピュータのＵＳＢポートに接続されるＵＳＢキーにおいて、ＵＳＢポートにＵＳＢキーが差し込まれた状態で、コンピュータに搭載されているブラウザー又はメーラー若しくは双方のセキュリティに関する設定ファイルを退避し、予め用意されたセキュリティを向上させる設定ファイルに変更し、ＵＳＢキーをＵＳＢポートから抜き出す際の処理において変更した設定ファイルを前記退避した設定ファイルに戻すコンピュータプログラムを記録するものであり、当該ＵＳＢキーでブラウザー、メーラーの設定ファイルを容易にセキュリティを向上させるための設定ファイルに変更でき、更にＵＳＢキーを抜き出す際には、設定を簡単に元に戻すことができる。

【０００７】本発明は、上記ＵＳＢキーにおいて、変更可能な設定ファイルが、ユーザの指定により設定事項を

4

セキュリティの程度に応じて変更可能としたものであり、セキュリティの程度によって細かく設定事項をユーザが指定できる。

【０００８】本発明は、コンピュータのＵＳＢポートに接続されるＵＳＢキーにおいて、ＵＳＢポートにＵＳＢキーが差し込まれた状態で、コンピュータに搭載されたＯＳの状態をチェックし、当該ＯＳに関する情報を予め記憶するＵＲＬのサイトに接続し、その情報を当該サイトのウェブサーバに出力するコンピュータプログラムを記憶するものであり、ＵＳＢキーが挿入されたコンピュータのＯＳの状態をウェブサーバに容易に提供できる。

【０００９】本発明は、セキュリティ保全システムにおいて、上記ＵＳＢキーから提供されたＯＳに関する情報に対して、ウェブサーバが、当該ＯＳのセキュリティホールに最新のパッチが当てられているか否かを診断し、最新のパッチが当てられていればその旨を表示し、最新のパッチが当てられていなければ当該パッチを当てるためのガイダンスを表示するものであり、ウェブサーバによるコンピュータのＯＳの状態を診断することで、ユーザはコンピュータの安全性を容易に認識でき、コンピュータを常に最新のセキュリティ状態としておくことができる。

【００１０】本発明は、上記セキュリティ保全システムにおいて、ＵＳＢキーがコンピュータのＵＳＢポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはＵＳＢキー内のＵＲＬにアクセスしてＯＳに関する情報をウェブサーバに提供するものであり、コンピュータの電源オン時には必ずＯＳの状態が診断され、コンピュータのセキュリティを向上させることができる。

【００１１】本発明は、上記セキュリティ保全システムにおいて、ウェブサーバが、表示の際に、セキュリティホールに関する情報、コンピュータウィルス及びワクチンソフトに関する情報も表示するものであり、ユーザはコンピュータの安全性を容易に認識できるだけでなく、セキュリティに関連する情報もウェブサイトから得ることができる。

【００１２】本発明は、コンピュータのＵＳＢポートに接続されるＵＳＢキーであって、ＵＳＢポートにＵＳＢキーが差し込まれた状態で、コンピュータに搭載されているブラウザー又はメーラー若しくは双方のセキュリティに関する設定ファイルをコピーし、当該ＵＳＢキー内に記憶するＵＲＬにアクセスして当該コンピュータのＯＳに関する情報及びコピーした設定ファイルをウェブサーバに提供し、ＯＳに関する情報とコピーした設定ファイルからウェブサーバが用意したセキュリティに関する設定ファイルをコンピュータで使用可能とするコンピュータプログラムを記録するものであり、コンピュータのＯＳの状態とセキュリティの設定ファイルの内容から適正な設定ファイルをウェブサーバより取得できる。

【００１３】本発明は、セキュリティ保全システムにおいて、請求項７記載のＵＳＢキーから提供されたＯＳに関する情報及びコピーした設定ファイルに対して、当該ＯＳに関する情報に対して当該コピーした設定ファイルがセキュリティ確保できる内容であるか判断し、セキュリティ確保できないものであれば、セキュリティ確保できる設定ファイルをコンピュータに対して提供するウェブサーバを有するものであり、コンピュータにおけるセキュリティをチェックしてセキュリティを確保できる。

【００１４】本発明は、上記セキュリティ保全システムにおいて、ＵＳＢキーがコンピュータのＵＳＢポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはＵＳＢキー内に記憶するＵＲＬにアクセスしてＯＳに関する情報及びコピーしたセキュリティに関する設定ファイルをウェブサーバに提供するものであり、コンピュータの電源オン時には必ずＯＳの状態及びセキュリティに関する設定ファイルの内容が診断され、コンピュータのセキュリティを向上させることができる。

【００１５】本発明は、上記ＵＳＢキーにおいて、変更する設定ファイルの設定内容は、規定値としてセキュリティが最高レベルとなるよう設定されているものであり、コンピュータウィルス感染を防止できる。

【００１６】本発明は、上記ＵＳＢキーにおいて、新規プロセスが発生すると、当該プロセスがレジストリに正規に登録されているか否かを検索し、正規に登録されていれば当該プロセスを動作させ、正規に登録されていなければ当該プロセスを動作させないプロセス監視機能を備えたものであり、コンピュータウィルス感染を防止できる。

【００１７】本発明は、上記ＵＳＢキーにおいて、ＯＳに関する情報の問い合わせに対してＯＳに関する情報の出力を停止するロック機能を備えたものであり、コンピュータウィルスの侵入を防止できる。

【００１８】本発明は、上記ＵＳＢキーにおいて、特定サイトにアクセスし、ファイルのウィルス感染をチェックし、当該ファイルをオンラインバックアップする機能を備えたものであり、コンピュータウィルス感染が予想されるファイルをチェックでき、感染の予想される若しくは感染したファイルをオンラインで外部に記憶させることで、コンピュータを保全できる。

【００１９】本発明は、上記ＵＳＢキーにおいて、コンピュータのシステム領域への不正アクセスを禁止する機能と、新規ファイルの自動作成を禁止する機能と、コンピュータの記憶装置内のファイルへの不正アクセスを禁止する機能とを備えたものであり、コンピュータウィルス感染を防止できる。

【００２０】本発明は、上記ＵＳＢキーにおいて、コンピュータのメモリ常駐を不許可とした上で、ファイル内容をテキストに変換してコンピュータで表示させる機能を備えたものであり、コンピュータウィルスに感染したファイルの内容をテキストで確認できる。

【００２１】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら説明する。本発明の実施の形態に係るＵＳＢキーは、パソコン（ＰＣ）に搭載されたブラウザー及びメーラーの設定を、コンピュータウィルスの侵入を防止するよう変更するプログラムを記憶しており、ＵＳＢポートにそのＵＳＢキーが差し込まれている時は、そのプログラムに従ってＰＣが動作してブラウザー等の設定を変更し、ＵＳＢキーを抜き出す際には、変更前の設定に戻すものであり、ＵＳＢキー挿入時に設定変更を容易に行い、セキュリティを向上させることができるものである。

【００２２】また、本発明の実施の形態に係るＵＳＢキーを用いたセキュリティ保全システムは、ＵＳＢキー内のプログラムがＰＣの状態をチェックしてＷｅｂサーバ３に出力し、Ｗｅｂサーバ３は、当該ＰＣ状態に応じて最新のパッチが当てられているか否かを診断してＰＣ向けに表示し、パッチが当てられていなければガイダンスに従ってパッチを当てるよう促すようにしているので、ユーザはＰＣの最新状況を知ることができ安心であり、また、ガイダンスに従うと容易にパッチを当てることがでできるものである。

【００２３】本発明の実施の形態に係るセキュリティ保全システムの構成について図１を参照しながら説明する。図１は、本発明の実施の形態に係るセキュリティ保全システムの構成ブロック図である。本発明の実施の形態に係るセキュリティ保全システム（本システム）は、図１に示すように、ＵＳＢキー１と、パソコン（ＰＣ）２と、ウェブ（Ｗｅｂ）サーバ３とを有している。ＵＳＢキー１は、ＰＣ２のＵＳＢポートに挿入されるものである。ＰＣ２は、インターネットを介してＷｅｂサーバ３に接続可能となっている。

【００２４】本システムにおける各部を具体的に説明する。ＵＳＢキー１は、以下に説明するプログラムとデータを記憶している。ＵＳＢキー１に記憶されているプログラムは、（１）ブラウザー及びメーラーの設定変更を行うためのプログラム、（２）Ｗｅｂサーバ３にアクセスするための制御を行うプログラム、（３）自ＰＣの状態をチェックし、その情報をＷｅｂサーバ３に出力するプログラムである。また、ＵＳＢキー１に記憶されているデータは、（１）ブラウザー及びメーラーの設定ファイル、（２）ＷｅｂサーバにアクセスするためのＵＲＬ（UniformResource Locator）であり、また、設定変更前の元の設定ファイルが一時的に記憶される。

【００２５】ＰＣ２は、ＵＳＢキー１内のプログラムを動作させるコンピュータで、ブラウザー及びメーラーの設定ファイルを変更し、また、自機のＯＳ状態をチェックして、その状態に関するデータを、インターネットを

7

介してＷｅｂサーバ３にアクセスして出力する。

【００２６】Ｗｅｂサーバ３は、ＯＳ提供会社のセキュリティホールに関する情報、コンピュータウィルス及びワクチンソフトに関する情報を提供する。また、Ｗｅｂサーバ３は、ＰＣ２からそのＯＳの状態に関するデータを受け取ると、そのＯＳが最新のセキュリティ状態となっているか否かを判断（診断）し、ＯＳ提供会社からパッチ用プログラムが提供されているにも拘わらず、そのＯＳにはパッチ用プログラムが当てられていない（最新のセキュリティ状態ではない）ものであると、パッチ用プログラムでパッチを当てる操作をＷｅｂ上でガイダンス表示する。

【００２７】従って、Ｗｅｂサーバ３は、ＰＣ２のＯＳの種類に応じて診断を行い、またＯＳの状態に応じたガイダンス表示を行う。ＰＣ２のユーザは、当該ガイダンスに従ってパッチ用プログラムをＰＣ２にダウンロードしてパッチを当てるようにすれば、初心者でも容易にその作業を行うことができる。

【００２８】次に、本システムの動作について図２～図４を参照しながら説明する。図２は、ブラウザー及びメーラーの設定変更の処理を示すフロー図であり、図３は、ＯＳ状態をチェックして提供する処理を示すフロー図であり、図４は、Ｗｅｂサーバ３における処理を示すフロー図である。

【００２９】図２に示すように、ＵＳＢキー１内のブラウザー及びメーラーの設定ファイルを変更するプログラムは、ＰＣ２内で起動し（Ｓ１）、設定変更用のインターフェースを表示する（Ｓ２）。次に、ＰＣ２のユーザによって設定指示の入力が行われ（Ｓ３）、現在の設定ファイルをＵＳＢキー１内に退避する（Ｓ４）。

【００３０】次に、処理Ｓ３における指示に従って変更された設定ファイルで書き替える（Ｓ５）。書き替えは、予めＵＳＢキー１内に変更用の設定ファイルが記憶されており、処理Ｓ３によってユーザがセキュリティの程度に応じて設定事項を指定して変更用の設定ファイルを作成し、その変更用の設定ファイルとブラウザー等に既に記憶されている設定ファイルとを置き換えるというものである。

【００３１】そして、ＰＣ２からプログラム終了の指示が入力されると（Ｓ６）、処理Ｓ４でＵＳＢキー１内に退避した元の設定ファイルに戻す処理を行う（Ｓ７）。そして、プログラムが終了する（Ｓ８）。このようにして、ＰＣ２内のブラウザー及びメーラーの設定ファイルの変更を初心者でも容易に行うことができる。

【００３２】次に、図３を用いてＰＣ２のＯＳ状態チェック及びそのデータの提供について説明する。図３に示すように、ＵＳＢキー１内のＯＳ状態チェック及びデータ提供のプログラムが起動されると（Ｓ１１）、ＯＳの状態をチェックする（Ｓ１２）。ＯＳ状態チェックは、当該プログラムがＯＳの種類、バージョンアップされた

8

ファイル等を参照し、ＰＣ２の現在のＯＳに関するデータ（ＰＣ状態情報）を取得し、ＵＳＢキー１内に一時的に記憶する。

【００３３】そして、ＰＣ２は、ＵＳＢキー１内に記憶しているＵＲＬにインターネット経由でアクセスし（Ｓ１３）、Ｗｅｂサーバ３に一時的に記憶したＰＣ状態情報を提供する（Ｓ１４）。これで、ＰＣ２側の処理を終了する（Ｓ１５）。ここで、Ｗｅｂサーバ３へのアクセスは、ＰＣ２にＵＳＢキー１が挿入された状態で、ＰＣ２の電源がオンになると、自動的に行うようにしてもよいし、ＰＣ２でＵＳＢキー１内のプログラムを起動して手動にて行うようにしてもよい。

【００３４】次に、ＰＣ２からＰＣ状態情報を入力したＷｅｂサーバ３の処理について図４を用いて説明する。図４に示すように、ＰＣ２からＰＣ状態情報を入力したＷｅｂサーバ３は処理を開始し（Ｓ２１）、ＰＣ状態情報に示されたＰＣ状態（当該ＰＣのＯＳの状態）に応じた情報を参照する（Ｓ２２）。具体的には、提供されるＰＣ状態情報からＯＳの種類、バージョンアップ状況を認識し、当該ＰＣにおける現在のＯＳに関するセキュリティホール及びパッチに関する情報を参照する。

【００３５】そして、ＰＣ状態情報からＰＣ２におけるＯＳの全てのセキュリティホールにパッチが当てられているか否かを判断（診断）し（Ｓ２３）、パッチが当てられていなければ（Ｎｏの場合）、パッチが当てられていないセキュリティホールにパッチを当てるガイダンスを出力し（Ｓ２４）、そのガイダンスに従ってユーザにはパッチ当てを行わせる。また、パッチが当てられていれば（Ｙｅｓの場合）、パッチが当てられている旨をＰＣ２向けに表示する（Ｓ２５）。

【００３６】このように、ＰＣ２は、ＵＳＢキー１が差し込まれている状態であれば、Ｗｅｂサーバ３にアクセスして当該ＰＣの状態を報告し、Ｗｅｂサーバ３では、報告（提供）されたＰＣ状態から現在の状況が最新の状態にてパッチが当てられているか否かを知らせることができ、パッチが当てられていなければ、操作ガイダンスに従ってパッチを当てる作業を容易に行うことができる。つまり、ユーザは、ＰＣ２のＯＳに対して安全性を容易に認識できるものである。

【００３７】尚、Ｗｅｂサーバ３にアクセスした時には、ＰＣ２の状態の診断結果を表示するだけでなく、関連するコンピュータウィルス及びワクチンソフトウェアの最新情報も表示すると、ＰＣユーザにとってネットワークのセキュリティ関連の最新情報を知ることができて便利である。

【００３８】また、本発明の別の実施の形態に係るセキュリティ保全システム（別のシステム）について説明する。この別のシステムは、構成としては図１のものと同様であるが、ＵＳＢキー１内のプログラムの動作が本システムのものと異なっている。別のシステムは、ＵＳＢ

キー１がＰＣ２に挿入された状態で、ＵＳＢキー１内のプログラムを動作させると、そのプログラムがＵＳＢキー１内に記述されたＵＲＬ及びＵＳＢキー１の装置ＩＤを読み込み、更にＰＣ２におけるＯＳに関する情報とセキュリティに関する設定ファイルのコピーを読み込み、上記ＵＲＬの示すサイトにアクセスしてＵＳＢキーの装置ＩＤ、ＯＳに関する情報及び設定ファイルのコピーを送信する。

【００３９】サイトを管理するサーバ３は、ＰＣ２から受信したＵＳＢキー１の装置ＩＤから登録されたユーザを特定し、サーバ３で管理するユーザのＯＳに関する情報と受信したＯＳに関する情報とを比較し、ＯＳの状態に変化があったか否かをチェックする。

【００４０】また、サーバ３は、受信した設定ファイルのコピーを参照し、ＯＳの状態の関係からセキュリティ上で問題のない設定ファイルであるか否かチェックする。セキュリティ上問題があれば、適正な設定ファイルをＰＣ２にダウンロード可能とする。若しくは、適正な設定ファイルの内容となるようサイト上でガイダンス表示を行い、ユーザ自身に設定ファイルの内容を変更させることもできる。

【００４１】別のシステムにおけるＵＳＢキー１内に記憶された起動プログラムについて図５を参照しながら説明する。図５は、本発明の実施の形態に係る別のセキュリティ保全システムのＵＳＢキー内における起動プログラムの処理の流れを示すフローチャートである。別のシステムにおけるＵＳＢキー１に記憶された起動プログラムは、図５に示すように、起動される（Ｓ３１）と、ＵＳＢキー１内に記憶されたＵＲＬ、ＵＳＢキー１内の装置ＩＤを読み込み（Ｓ３２）、更にＰＣ２のハードディスクにアクセスしてＯＳに関する情報を取得し（Ｓ３３）、セキュリティの設定ファイルをコピーする（Ｓ３４）。

【００４２】次に、プログラムは、読み込んだＵＲＬでサーバ３へのアクセスを行い（Ｓ３５）、サーバ３へ装置のＩＤ、ＯＳに関する情報、それにコピーした設定ファイルを提供する（Ｓ３６）。

【００４３】そして、プログラムは、サーバ３から提供された設定ファイルをダウンロードして（Ｓ３７）、ＵＳＢキー１内に記憶する。このようにして、サーバ３に対する処理を終了する（３８）。

【００４４】そして、プログラムは、ＰＣ２内に設定されているセキュリティの設定ファイルを退避し、そのダウンロードした設定ファイルを用いてインターネットへのアクセス、またメールの送受信を行う。

【００４５】これに対して、サーバ３での処理について図６を参照しながら説明する。図６は、本発明の別の実施の形態に係るセキュリティ保全システムにおけるサーバ３での処理の流れを示すフローチャートである。サーバ３は、図６に示すように、ＰＣ２からアクセスされ（Ｓ４１）、装置ＩＤ、ＯＳに関する情報、セキュリティの設定ファイルのコピーを受信する（Ｓ４２）と、当該装置ＩＤからユーザを特定し（Ｓ４３）、サーバ３で管理するユーザのＯＳに関する情報と受信したＯＳに関する情報を比較し（Ｓ４４）、一致するか否かの判定を行う（Ｓ４５）。

【００４６】ＯＳのバージョンアップが為されていれば、不一致が生じるので、不一致の場合（Ｎｏの場合）、サーバ３で管理しているユーザのＯＳに関する情報を受信したＯＳに関する情報で更新する（Ｓ４６）。尚、一致する場合（Ｙｅｓの場合）、情報の更新は行わない。

【００４７】次に、不一致の場合に更新されたＯＳに関する情報、若しくは一致の場合は更新されないＯＳに関する情報に基づいて、サーバ３はセキュリティの設定ファイルの内容を参照し、当該ＯＳに対する十分なセキュリティが確保されているか判断する（Ｓ４７）。その設定ファイルでセキュリティが確保されていれば（Ｙｅｓの場合）、ユーザのＰＣ２の画面に十分なセキュリティであり、ダウンロード不要の旨を表示させる（Ｓ４８）。十分なセキュリティが確保されていなければ（Ｎｏの場合）、セキュリティが確保された安全な設定ファイルをユーザのＰＣ２にダウンロード可能に提供する（Ｓ４９）。そして、処理を終了する。

【００４８】上記別のシステムでは、ＰＣ２で現在使用されているセキュリティの設定ファイルをそのＯＳに関する情報との関連でセキュリティが確保されているか否かをサーバ３が判断しているので、ＵＳＢキー１を装着したＰＣ２では、現在の利用状況に対するセキュリティを確保でき、新たに登場するＯＳのセキュリティホールを突いた攻撃に対応できる。

【００４９】尚、上記別のシステムでは、ＵＳＢキー１内のプログラムをユーザが動作させることでセキュリティの確保を実現しているが、ＰＣ２にＵＳＢキー１が挿入された状態でＰＣ２が電源オンとなった時に、オートラン機能を用いて自動的に当該プログラムを起動するようにしてもよい。これにより、ＰＣ２の電源投入（オン）時に、ＰＣ２のＯＳの状態及び設定ファイルの内容を診断でき、セキュリティ確保された設定ファイルをＰＣ２に提供可能となるものである。

【００５０】また、ＯＳに関する情報との関係で、サーバ３に提供したコピーのセキュリティに関する設定ファイルでは十分なセキュリティを確保できない場合に、安全な設定ファイルに置き換えられるようダウンロード可能としているが、サーバ３のサイトの画面上で、ユーザがセキュリティ関連の項目を選択しながらセキュリティの設定ファイルを作成するようにしてもよい。

【００５１】尚、上記処理では、プログラムがサーバ３にセキュリティの設定ファイルのコピーを送信するようにしているが、コピーを送信せず、ＯＳに関する情報だ

けで、対応するセキュリティの設定ファイルをダウンロード可能としてもよい。

【００５２】

【実施例】次に、本発明の実施の形態に係るＵＳＢキーの一実施例を説明する。ＵＳＢキー１には、ＰＣ２のＵＳＢポートに差し込んだ際に、セキュリティ設定に関するプログラムが自動的に起動するようプログラム化されている。自動起動によって図７に示す画面が表示される。図７は、本発明の実施の形態に係るセキュリティ設定の画面の概略図である。

【００５３】図７に示すように、セキュリティ設定の画面は、複数のセキュリティに関する「チェックボックス」「セキュリティの選択バー」、それに「tmp read」「拡張機能」「終了」のボタンが表示される。チェックボックスの「マクロ」は、オフィスソフトの機能を制限し、マクロ型ウィルスの感染を防止するためのものであり、「スプリクト」は、Java（登録商標）スクリプトとVBスクリプトの動作を制限するためのものであり、「JAVA（登録商標）」は、その機能を停止するためのものであり、「cookie（登録商標）」は、その全ての機能を停止するためのものであり、「memory」は、不正メモリアクセスを禁止するためのものである。

【００５４】また、「セキュリティの選択バー」は、バーを「高」又は「低」方向に動かすことで、チェックボックスの設定を自動的に行うものである。例えば、選択バーが「低」であれば、チェックボックスの全てを制限しないよう設定し、選択バーを「高」に動かすことで、「マクロ」「スクリプト」の順に機能制限を設定し、選択バーが「高」でチェックボックスの全てを制限する設定にするものである。

【００５５】セキュリティ設定の規定値は、選択バーが「高」の位置、すなわち、チェックボックスの全ての機能が制限された状態としている。これにより、ウィルス対策が万全となるものである。

【００５６】また、セキュリティ設定画面における「tmp read」とは、ウィルスに感染していると思われるファイルの内容をテキストに変換して表示する機能である。この機能を実行する際には、（１）システム領域への不正アクセスを禁止し、（２）新規ファイルの自動作成を禁止し、（３）ハードディスク（ＨＤＤ）等の記憶装置内のファイルへの不正アクセスを禁止して、メモリ常駐を不許可とした上で、対象ファイルの内容をテキストとして表示するものである。

【００５７】上記（１）～（３）の禁止機能は、本実施例のＵＳＢキー１の基本機能であり、ＵＳＢキー１をＰＣ２のＵＳＢポートに差し込んだ時に、それら機能が動作するようになっている。この３つの禁止機能によって、ウィルス感染を防止している。

【００５８】次に、ＵＳＢキー１の別の機能を説明する。ＵＳＢキー１のセキュリティ関連のプログラムには、プロセス監視機能を備えている。プロセス監視機能とは、正規にレジストリに登録されたプログラムをチェックし、新規プロセスが発生すると、レジストリ内をサーチし、正規プロセスか否かを判定し、正規プロセスでなければ、そのプロセスを動作させないようにしたものである。これにより、正規でないプロセスの動作を停止でき、ウィルス感染を防止できる。

【００５９】また、ＵＳＢキー１のセキュリティ関連のプログラムには、ロック機能を備えている。ロック機能とは、ウィルスが侵入してくる際に、ＰＣ２のＯＳのバージョン情報を問い合わせてくることがあるが、その問い合わせにＯＳ情報を提供しないようにロックするものである。これにより、ウィルス侵入を防止できる。

【００６０】また、ＵＳＢキー１のセキュリティ関連のプログラムには、メールに添付されたファイルやユーザが指定したファイルのウィルス感染をインターネットの特定サイトにアクセスしてチェックを行い、そのファイルをオンラインバックアップする機能を備えている。この機能は、図７における「拡張機能」に含まれるものである。これにより、ウィルス感染の予想されるファイルをチェックでき、感染の予想される若しくは感染したファイルをオンラインで外部に記憶させることができ、ＰＣ２を安全に保つことができる。

【００６１】また、「拡張機能」の一つとして、オンラインウィルス駆除の機能がある。この機能を選択すると、特定サイトにオンラインアクセスし、ＰＣ２のウィルス駆除を行い、レポートを提供するものである。

【００６２】また、ＵＳＢキー１のセキュリティ関連のプログラムには、最新のシステムとワクチンに関する情報を提供するサイトにアクセス可能となっており、そのサイトのガイダンスに従うと簡単な操作でシステムとワクチンの更新ができるようになっている。

【００６３】

【発明の効果】本発明によれば、ＵＳＢポートにＵＳＢキーが差し込まれた状態で、コンピュータに搭載されているブラウザー又はメーラー若しくは双方のセキュリティに関する設定ファイルを退避し、予め用意されたセキュリティを向上させる設定ファイルに変更し、ＵＳＢキーをＵＳＢポートから抜き出す際の処理において変更した設定ファイルを前記退避した設定ファイルに戻すコンピュータプログラムを記録するＵＳＢキーとしているので、当該ＵＳＢキーでブラウザー、メーラーの設定ファイルを容易にセキュリティを向上させるための設定ファイルに変更でき、更にＵＳＢキーを抜き出す際には、設定を簡単に元に戻すことができる効果がある。

【００６４】本発明によれば、変更可能な設定ファイルが、ユーザの指定により設定事項をセキュリティの程度に応じて変更可能とした上記ＵＳＢキーとしているので、セキュリティの程度によって細かく設定事項をユーザが指定できる効果がある。

【００６５】本発明によれば、ＵＳＢポートにＵＳＢキーが差し込まれた状態で、コンピュータに搭載されたＯＳの状態をチェックし、当該ＯＳに関する情報を予め記憶するＵＲＬのサイトに接続し、その情報を当該サイトのウェブサーバに出力するコンピュータプログラムを記憶するＵＳＢキーとしているので、ＵＳＢキーが挿入されたコンピュータのＯＳの状態をウェブサーバに容易に提供できる効果がある。

【００６６】本発明によれば、上記ＵＳＢキーから提供されたＯＳに関する情報に対して、ウェブサーバが、当該ＯＳのセキュリティホールに最新のパッチが当てられているか否かを診断し、最新のパッチが当てられていればその旨を表示し、最新のパッチが当てられていなければ当該パッチを当てるためのガイダンスを表示するセキュリティ保全システムとしているので、ウェブサーバによるコンピュータのＯＳの状態を診断することで、ユーザはコンピュータの安全性を容易に認識でき、コンピュータを常に最新のセキュリティ状態としておくことができる効果がある。

【００６７】本発明によれば、ＵＳＢキーがコンピュータのＵＳＢポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはＵＳＢキー内のＵＲＬにアクセスしてＯＳに関する情報をウェブサーバに提供する上記セキュリティ保全システムとしているので、コンピュータの電源オン時には必ずＯＳの状態が診断され、コンピュータのセキュリティを向上させることができる効果がある。

【００６８】本発明によれば、ウェブサーバが、表示の際に、セキュリティホールに関する情報、コンピュータウィルス及びワクチンソフトに関する情報も表示する上記セキュリティ保全システムとしているので、ユーザはコンピュータの安全性を容易に認識できるだけでなく、セキュリティに関連する情報もウェブサイトから得ることができる効果がある。

【００６９】本発明によれば、コンピュータのＵＳＢポートに接続されるＵＳＢキーであって、ＵＳＢポートにＵＳＢキーが差し込まれた状態で、コンピュータに搭載されているブラウザー又はメーラー若しくは双方のセキュリティに関する設定ファイルをコピーし、当該ＵＳＢキー内に記憶するＵＲＬにアクセスして当該コンピュータのＯＳに関する情報及びコピーした設定ファイルをウェブサーバに提供し、ＯＳに関する情報とコピーした設定ファイルからウェブサーバが用意したセキュリティに関する設定ファイルをコンピュータで使用可能とするコンピュータプログラムを記録するものであり、コンピュータのＯＳの状態とセキュリティの設定ファイルの内容から適正な設定ファイルをウェブサーバより取得できる効果がある。

【００７０】本発明によれば、請求項７記載のＵＳＢキーから提供されたＯＳに関する情報及びコピーした設定ファイルに対して、当該ＯＳに関する情報に対して当該コピーした設定ファイルがセキュリティ確保できる内容であるか判断し、セキュリティ確保できないものであれば、セキュリティ確保できる設定ファイルをコンピュータに対して提供するウェブサーバを有するセキュリティ保全システムとしているので、コンピュータにおけるセキュリティをチェックしてセキュリティを確保できる効果がある。

【００７１】本発明によれば、ＵＳＢキーがコンピュータのＵＳＢポートに差し込まれている状態で、当該コンピュータの電源がオンとなると、コンピュータはＵＳＢキー内に記憶するＵＲＬにアクセスしてＯＳに関する情報及びコピーしたセキュリティに関する設定ファイルをウェブサーバに提供する上記セキュリティ保全システムとしているので、コンピュータの電源オン時には必ずＯＳの状態及びセキュリティに関する設定ファイルの内容が診断され、コンピュータのセキュリティを向上させることができる効果がある。

【００７２】本発明によれば、変更する設定ファイルの設定内容は、規定値としてセキュリティが最高レベルとなるよう設定されている上記ＵＳＢキーとしているので、コンピュータウィルス感染を防止できる効果がある。

【００７３】本発明によれば、新規プロセスが発生すると、当該プロセスがレジストリに正規に登録されているか否かを検索し、正規に登録されていれば当該プロセスを動作させ、正規に登録されていなければ当該プロセスを動作させないプロセス監視機能を備えた上記ＵＳＢキーとしているので、コンピュータウィルス感染を防止できる効果がある。

【００７４】本発明によれば、ＯＳに関する情報の問い合わせに対してＯＳに関する情報の出力を停止するロック機能を備えた上記ＵＳＢキーとしているので、コンピュータウィルスの侵入を防止できる効果がある。

【００７５】本発明によれば、特定サイトにアクセスし、ファイルのウィルス感染をチェックし、当該ファイルをオンラインバックアップする機能を備えた上記ＵＳＢキーとしているので、ウィルス感染が予想されるファイルをチェックでき、コンピュータウィルス感染の予想される若しくは感染したファイルをオンラインで外部に記憶させることで、コンピュータを保全できる効果がある。

【００７６】本発明によれば、コンピュータのシステム領域への不正アクセスを禁止する機能と、新規ファイルの自動作成を禁止する機能と、コンピュータの記憶装置内のファイルへの不正アクセスを禁止する機能とを備えた上記ＵＳＢキーとしているので、コンピュータウィルス感染を防止できる効果がある。

【００７７】本発明によれば、コンピュータのメモリ常駐を不許可とした上で、ファイル内容をテキストに変換

15

してコンピュータで表示させる機能を備えた上記ＵＳＢキーとしているので、コンピュータウィルスに感染したファイルの内容をテキストで確認できる効果がある。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るセキュリティ保全システムの構成ブロック図である。

【図２】ブラウザー及びメーラーの設定変更の処理を示すフロー図である。

【図３】ＯＳ状態をチェックして提供する処理を示すフロー図である。

【図４】Ｗｅｂサーバ３における処理を示すフロー図である。

16

【図５】本発明の実施の形態に係る別のセキュリティ保全システムのＵＳＢキー内における起動プログラムの処理の流れを示すフローチャートである。

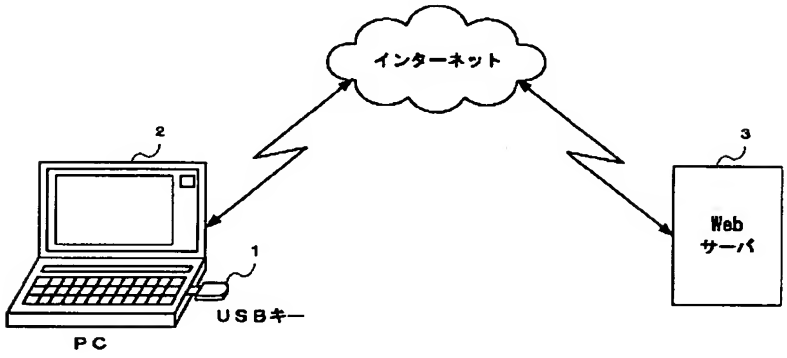
【図６】本発明の別の実施の形態に係るセキュリティ保全システムにおけるサーバでの処理の流れを示すフローチャートである。

【図７】本発明の実施の形態に係るセキュリティ設定の画面の概略図である。

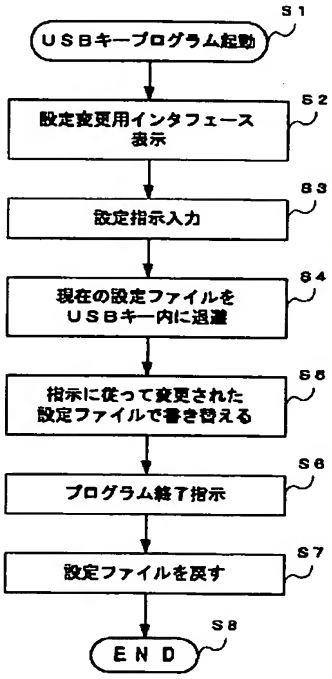
【符号の説明】

１…ＵＳＢキー、　２…ＰＣ、　３…Ｗｅｂサーバ

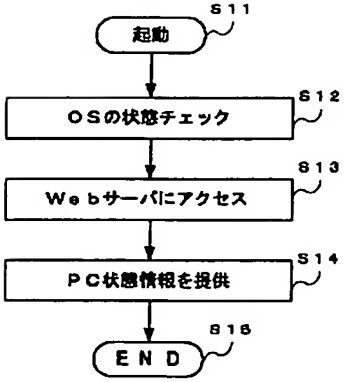
【図１】



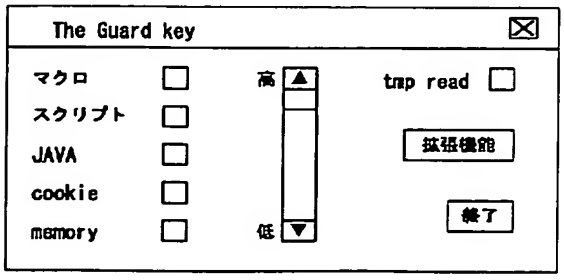
【図２】



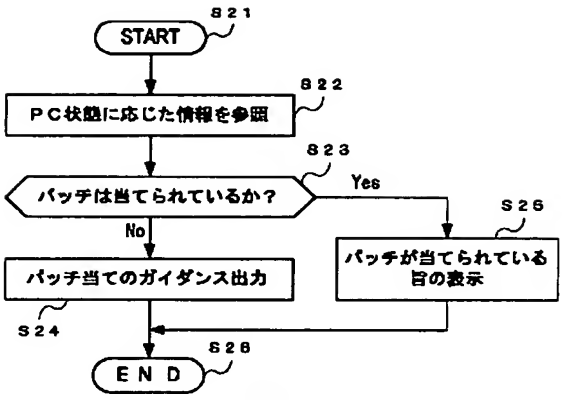
【図３】



【図７】

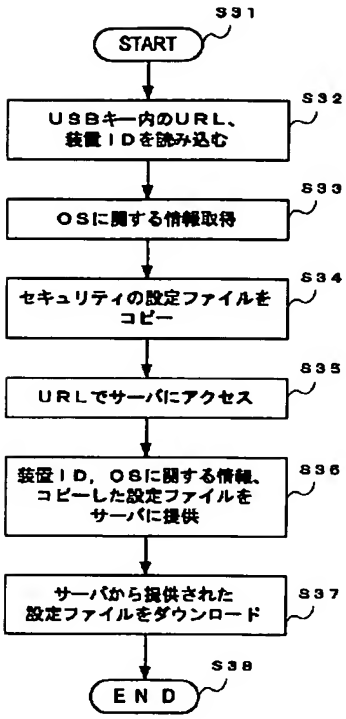


【図４】


S21
START
S22
PC状態に応じた情報を参照
S23
パッチは当てられているか？
Yes
No
S26
パッチが当てられている旨の表示
パッチ当てのガイダンス出力
S24
S28
END

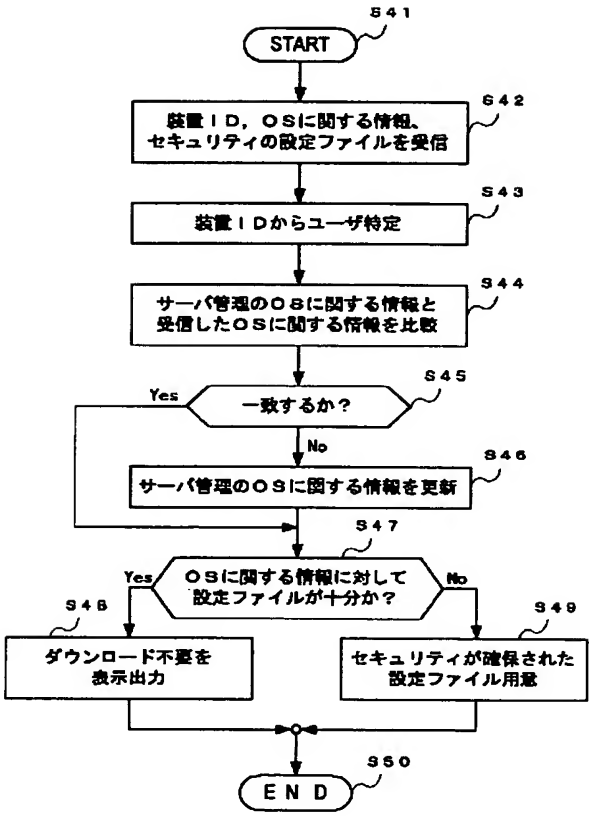
【図4】

【図５】


S31
START
S32
USBキー内のURL、装置IDを読み込む
S33
OSに関する情報取得
S34
セキュリティの設定ファイルをコピー
S35
URLでサーバにアクセス
S36
装置ID，OSに関する情報、コピーした設定ファイルをサーバに提供
S37
サーバから提供された設定ファイルをダウンロード
S38
END

【図5】

【図６】


S41
START
S42
装置ＩＤ，ＯＳに関する情報、
セキュリティの設定ファイルを受信
S43
装置ＩＤからユーザ特定
S44
サーバ管理のＯＳに関する情報と
受信したＯＳに関する情報を比較
S45
Yes
一致するか？
No
S46
サーバ管理のＯＳに関する情報を更新
S47
Yes
ＯＳに関する情報に対して
設定ファイルが十分か？
No
S48
ダウンロード不要を
表示出力
S49
セキュリティが確保された
設定ファイル用意
S50
ＥＮＤ

【図６】